Содержание

Введение

Даже самая совершенная система защиты бесполезна, если ей управляет психологически неустойчивый, наивный или доверчивый человек. Помните анекдот о диссертации на тему "зависимость скорости перебора паролей от температуры паяльника (утюга)"? Многие почему-то забывают, что в роли объекта атаки может выступать не только машина, но и ее оператор. Причем, оператор зачастую оказывается слабейшим звеном в системе защиты.

На хакерском жаргоне атака на человека называется *социальной инженерией* (*social engineering*) и в своем каноническом виде обычно сводится к звонкам по телефону с целью получения конфиденциальной информации (как правило, паролей) посредством выдачи себя за другое лицо.

В данной статье термин "социальная инженерия" рассматривается намного шире и обозначает любые способы психологического воздействия на человека, как то: введение в заблуждение (обман), игра на чувствах (любви, ненависти, зависти, алчности, в том числе и шантаж).

Собственно, подобные приемы не новы и известны еще со времен глубокой древности. Остается только удивляться тому, что за истекшие тысячелетия человечество так и не научилось противостоять мошенникам и отличать правду ото лжи. Еще удивительнее то, что арсенал злоумышленников не претерпел никаких принципиальных изменений. Напротив, с развитием коммуникационных технологий их задача значительно упростилась.

Общаясь по Интернет, вы не видите и не слышите своего собеседника, более того, нет никаких гарантий, что сообщение действительно отправлено тем адресатом, имя которого стоит в заголовке. Атакующий может находиться и в соседней комнате, и в соседнем городе, и даже на соседнем континенте!

Все это значительно усложняет идентификацию личности, поиск и доказательство причастности злоумышленника к атаке. Стоит ли удивляться огромной популярности социальной инженерии среди молодежи?

К счастью, подавляющее большинство мошенников действует по идентичным или близким шаблонам. Поэтому, изучение приемов их "работы" позволяет распознать обман и не попасться на удочку. Автором этой статьи собрана обширная коллекция хакерского арсенала, наиболее популярные "экспонаты" которой представлены ниже. Конечно, на исчерпывающее руководство по обеспечению собственной безопасности данная публикация не претендует, но общее представление о методиках хищения денег или информации все же дает.

1. Определение понятия социальная инженерия

Социальная инженерия — это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным. Зачастую социальную инженерию рассматривают как незаконный метод получения информации, однако это не совсем так. Социальную инженерию можно также использовать и в законных целях, и не только для получения информации, а и для совершения действий конкретным человеком. Сегодня социальную инженерию зачастую используют в интернете, для получения закрытой информации, или информации, которая представляет большую ценность.

Социальная инженерия - совокупность подходов в прикладных социальных науках, ориентированных:
- на изменение поведения и установок людей;
- на разрешение социальных проблем;
- на адаптацию социальных институтов к изменяющимся условиям;
- на сохранение социальной активности.

Злоумышленник получает информацию, например, путем сбора информации о служащих объекта атаки, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего.

Злоумышленник может позвонить работнику компании (под видом технической службы) и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе. Очень часто этот трюк проходит.

Имена служащих удается узнать после череды звонков и изучения имён руководителей на сайте компании и других источников открытой информации (отчётов, рекламы и т. п.).

Используя реальные имена в разговоре со службой технической поддержки, злоумышленник рассказывает придуманную историю, что не может попасть на важное совещание на сайте со своей учетной записью удаленного доступа.

Другим подспорьем в данном методе являются исследование мусора организаций, виртуальных мусорных корзин, кража портативного компьютера или носителей информации.

Данный метод используется, когда злоумышленник наметил в качестве жертвы конкретную компанию.

Социальная инженерия — относительно молодая наука, которая является составной частью социологии, и претендует на совокупность тех специфических знаний, которые направляют, приводят в порядок и оптимизируют процесс создания, модернизации и воспроизведения новых («искусственных») социальных реальностей. Определенным образом она «достраивает» социологическую науку, завершает ее на фазе преобразования научных знаний в модели, проекты и конструкции социальных институтов, ценностей, норм, алгоритмов деятельности, отношений, поведения и т. п. Занятия сориентированы на вооружение слушателей прежде всего методологией аналитико-синтетического мышления и знаниями формализованных процедур (технологий) конструкторско-изобретательской деятельности. В характеристике формализованных операций, из которых складывается это последнее, особое внимание обращается на операции сложной комбинаторики. Игнорирование принципа системности в операциях комбинаторики нанесли и продолжают наносить большой ущерб на всех уровнях трансформационных процессов, которые происходят в нашем

обществе. Последовательные знания принципиальных требований к указанным операциям дают основания к предотвращению ошибочных извращений в реформационной практике на ее макро-, мезо- и микроуровнях.

Несмотря на то, что понятие социальной инженерии появилось недавно, люди в той или иной форме пользовались ее техниками испокон веков. В той же Древней Греции и Риме в большом почете были люди, могущие навешать на уши любую лапшу и убедить собеседника в «очевидной неправоте». Выступая от имени верхов, они вели дипломатические переговоры, а, подмешивая в свои слова вранье, лесть и выгодные аргументы, нередко решали такие проблемы, которые, в противном случае, невозможно было решить без помощи меча. В среде шпионов социальная инженерия всегда являлась главным оружием. Выдавая себя за кого угодно, агенты КГБ и ЦРУ могли выведать самые страшные государственные тайны.

В начале 70-х гг., в период расцвета фрикинга, некоторые телефонные хулиганы забавлялись тем, что названивали с уличных автоматов операторам Ma Bell и подкалывали их на тему компетентности. Потом кто-то, очевидно, сообразил, что, если немного перестроить фразы и кое-где солгать, можно заставить тех. персонал не просто оправдываться, а выдавать в порыве эмоций конфиденциальную информацию. Фрикеры стали потихоньку экспериментировать с уловками и к концу 70-х настолько отработали техники манипулирования неподготовленными операторами, что могли без проблем узнать у них практически все, что хотели.

Заговаривать людям зубы по телефону, чтобы получить какую-то информацию или просто заставить их что-то сделать, приравнивалось к искусству. Профессионалы в этой области очень гордились своим мастерством. Самые искусные социальные инженеры (синжеры) всегда действовали экспромтом, полагаясь на свое чутье. По наводящим вопросам, по интонации голоса они могли определить комплексы и страхи человека и,

мгновенно сориентировавшись, сыграть на них. Если на том конце провода находилась молоденькая, недавно поступившая на работу девушка — фрикер намекал на возможные неприятности с боссом, если это был какой-то самоуверенный тюфяк — достаточно было представиться начинающим пользовтелем, которому все нужно показать и рассказать. К каждому подбирался свой ключ. С появлением компьютеров, многие фрикеры перебрались в компьютерные сети и стали хакерами. Навыки СИ в новой области стали еще полезнее. Если раньше мозги оператору пудрили в основном для получения кусочков информации из корпоративных справочников, то теперь стало возможным узнать пароль для входа в закрытую систему и скачать оттуда кучу тех же справочников или что-то секретное. Причем такой способ был намного быстрее и проще технического. Не нужно искать дыры в навороченной системе защиты, не надо ждать, пока Jack the Ripper угадает правильный пароль, не обязательно играть в кошки-мышки с админом. Достаточно позвонить по телефону и, при правильном подходе, на другом конце линии сами назовут заветное слово.

2.Виды социальной инженерии

Социальная инженерия подразделятся на два основных вида:

- Социальная инженерия.
- Обратная социальная инженерия.

У этих двух видов общее только то, что они воздействуют на человека, но при этом их способы воздействия совершенно различны. Социальная инженерия может быть применима в любой обстановке, без предварительной подготовки, а люди, в отношении которых была направлена социальная инженерия, остаются в неведении настоящей ситуации, иногда и личностей.

Социальная инженерия успешно применяется не только для взлома и получения информации, как написано во многих книгах, но и в реальных ситуациях, для извлечения обыкновенной прибыли.

В обычной жизни мы не взламываем ежедневно компьютеры и сервисы, но почти ежедневно тратим деньги, которые нужно как-то зарабатывать. Разберем самый обычный пример из жизни. Есть одна компания, под кодовым названием фирма №1. Как и у любой хорошей фирмы у нее много сайтов, на которых представлен один и тот же товар или услуга.

Поисковые системы, которые являются основным источником посетителей на сайт, пытаются сделать выдачу по определенному запросу как можно более разнообразной, чтобы получить еще больше посетителей, а, следовательно, денег.

Раньше одна и та же компания создавала от 10 до 50 сайтов, и старалась вывести их все на первую и вторую страницу в выдаче. И это получалось. В итоге человек обращался в одну и ту же фирму с одним и тем же заказом, не зависимо от того, какой бы он сайт не выбрал.

Почему человек думал, что это разные организации?

Потому что, это были разные сайты, поэтому он звонил, заказывал, иногда к нему даже приезжали люди как бы от разных фирм, но это перестало работать со временем.
Поисковые системы ввели фильтр (antiaffilat фильтр). При обнаружении сайтов одной фирмы, по одному запросу в выдаче, если будет выявлено, что целью организации является продажа товаров и оказание услуг, к этим сайтам будет применен специальный фильтр, который оставляет один сайт, а остальные отбрасывает на самые дальние странички.

Сейчас, чтобы противостоять этому фильтру, придумано много методов, один из которых – это скрытие данных владельца домена по запросу whois. Почту и телефон же стараются указывать для каждого домена разные. Тоже самое дело и с телефонами и адресами на самом сайте. Названия фирм очень часто пишут, в соответствии с названиями доменов. Например, для этого домена specialist-seo.ru фирма, скорее всего, называлась бы, ООО «Специалист СЕО».

Социальная инженерия применяется не только для обмана, но и в качестве способа ведения статистики. Пример, на сайте продаются дорогие автомобили. Под товаром какой-нибудь многоканальный телефон и подпись, «Спрашивайте Вашего персонального менеджера Ивана». Под другим товаром - «Спрашивайте Вашего персонального менеджера Александра» и т.п.

Рекомендуется указывать имена людей вообще не работающих в этой организации, чтобы точно вести статистику звонков посетителей с конкретных страничек или сайтов.

Реально таких людей даже не существует, а все звонки могут обрабатывать один – два человека. Но такие подписи придают солидность организации, повышают уровень доверия и используются в маркетинговых целях.

Социальная инженерия очень часто используются в целях повышения уровня доверия посетителя, причем повсеместно.

В интернет основными факторами, позволяющими повысить доверия к сайту являются следующие:

- Оформление сайта - однотипные оформления вызывают недоверие. Как, например, у всяких интернет пирамид, люди разные, а страницы по оформлению совершенно идентичны. Как правило это: большой

длинный текст, введением в который является мысль о том как будет хорошо или наоборот очень трудно достичь желаемого успеха и т.п. в начале и представлен яркий контраст с тем что будет потом, на этой же страничке обычно располагается почтовый адрес или форма подписки.

- Использование специальных подписей, кроме примера, приведенного выше, это ещё может быть указаниеподписи под обычным прямым сотовым номером, «Многоканальный телефон» и подобные записи
- Регистрация доменов второго уровня- применяется так как вызывает недоверия фирма, использующая бесплатный домен третьего уровня. Если у организации нет денег даже на домен 2 уровня, то о каких платных услугах может идти речь.
- Установка счетчиков с других сайтов, которые показывают посетителей другого сайта, их более 2-3 тыс., а реально Вы на этом сайте вообще первый человек сегодня.

Помимо выше приведённых примеров существует ещё масса других методик и способов.

Предположим , у нашей фирмы №1 есть следующее:

- Три сотовых телефона с прямыми городскими номерами
- Один домашний адрес
- Три сайта.

Каким же образом фирма будет получать прибыль от этого?

- На каждом сайте по whois указываются разные контактные данные, а имя и фамилия владельца скрывается.
- Сайты находятся на разных хостингах, чтобы обеспечить различные ip адреса.

- На всех сайтах указаны контакты и телефоны, которые не пересекаются и не повторяются.
- На каждом сайте уникальное оформление и содержание.

Осталось понять только одно, как фирма, находящаяся в собственной квартире доставляет товары и отправляет заказчиков на склады?

Все очень просто, рассказывать детали не буду. Дам только намек, что есть договоренность с производителями, которые и выполняют всю работу, а задача владельцев сайта, только сообщить, что клиент пришел от них.

Не стоит бояться заказывать через интернет, после прочтения данного текста, Вы просто делаете заказ через посредников, у которых есть определенные скидки, поэтому они могут предлагать товары дешевле, чем производитель, который специально фиксирует цены.

3.Техники и термины социальной инженерии

Все техники социальной инженерии основаны на особенностях принятия решений людьми, называемых когнитивным базисом. Они также могут быть названы особенностью принятия решения человеческой и социальной психологий, основанной на том, что человек должен кому-либо доверять в социальной среде воспитания.

3.1Претекстинг

Претекстинг — это действие, отработанное по заранее составленному сценарию (претексту). В результате цель должна выдать определённую информацию или совершить определённое действие. Этот вид атак применяется обычно по телефону. Чаще эта техника включает в себя больше, чем просто ложь, и требует каких-либо предварительных исследований (например, персонализации: дата рождения, сумма последнего счёта и др.), с

тем, чтобы обеспечить доверие цели. К этому же виду относятся атаки и по онлайн-мессенджерам, например, по ICQ.

3.2Фишинг

Фишинг — техника, направленная на жульническое получение конфиденциальной информации. Обычно злоумышленник посылает цели e-mail, подделанный под официальное письмо — от банка или платёжной системы — требующее «проверки» определённой информации или совершения определённых действий. Это письмо обычно содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и контентом, и содержащую форму, требующую ввести конфиденциальную информацию — от домашнего адреса до пин-кода банковской карты.

3.3Троянский конь

Эта техника эксплуатирует любопытство, либо алчность цели. Злоумышленник отправляет e-mail, содержащий во вложении «клёвый» или «сексуальный» скрин-сейвер, важный апгрейд антивируса или даже свежий компромат на сотрудника. Такая техника остаётся эффективной, пока пользователи будут слепо кликать по любым вложениям.

3.4Дорожное яблоко

Этот метод атаки представляет собой адаптацию троянского коня и состоит в использовании физических носителей. Злоумышленник может подбросить инфицированный CD или флэш в месте, где носитель может быть легко найден (туалет, лифт, парковка). Носитель подделывается под официальный и сопровождается подписью, призванной вызвать любопытство.

Пример: Злоумышленник может подбросить CD, снабжённый корпоративным логотипом и ссылкой на официальный сайт компании цели, и снабдить его надписью «Заработная плата руководящего состава Q1 2007». Диск может быть оставлен на полу лифта или в вестибюле. Сотрудник по незнанию может подобрать диск и вставить его в компьютер, чтобы удовлетворить своё любопытство, или просто «добрый самаритянин» отнесёт диск в компанию.

3.5Кви про кво

Злоумышленник может позвонить по случайному номеру в компанию и представиться сотрудником техподдержки, опрашивающим, есть ли какие-либо технические проблемы. В случае, если они есть, в процессе их «решения» цель вводит команды, которые позволяют хакеру запустить вредоносное программное обеспечение.

4.Обратная социальная инженерия

Этот недостаток пытается устранить обратная социальная инженерия или как часто пишется **ОСИ**.
Обратная социальная инженерия строится на трех факторах.

- Создание ситуации, которая вынуждает человека обратиться за помощью
- Реклама своих услуг или опережение оказания помощи другими людьми
- Оказание помощи и воздействие

В данном случае вначале нужно создать ситуацию, а для создания ситуации нужно изучить человека (или группу лиц), на которого будет оказываться воздействие.
Сейчас не проходят трюки, описанные ранее, замените название файла и т.п.

Все решается простой переустановкой программ, да и запустить программу в большинстве случаев не удастся, уже не те времена.

Остается один вариант. Исследовать людей, их интересы, пристрастия и пытаться воздействовать за счет них, причем программы и любые способы электронного воздействия должны быть полностью работоспособны и до определенного времени не вызывать никаких опасений.

Возьмем один из старых вариантов, описанных в большинстве книг. Пошлем по почте адресату новый диск его любимого исполнителя с записанным вирусом. Думаете, сработает? Очень сомневаюсь. Большинство проигрывателей запустит диск без запуска вируса, да и антивирус заблокирует такой вирус очень быстро.
Лучше всего не использовать такие методы, они просто не эффективны. Гораздо эффективнее разработать программу, которая будет полезна этому предприятию, разработана специально для него, но через определенное время ее нужно обслуживать, обновлять и так далее.

Вот вам и доступ и зависимость. О чем еще мечтать. Наверное, о том, чтобы научиться делать такие программы.

Таким образом, обратная социальная инженерия позволяет управлять людьми, но для этого нужно много сил и знаний. Социальная инженерия воздействует в большинстве своем на более широкую аудиторию и более выгодна, хотя Вы и находитесь в зависимом состоянии.

Целью обратной социальной инженерии (reverse social engineering) является заставить цель самой рассказать о своих паролях, информацию о компании.

Пример:

1. Фильм "Хакеры" когда главный герой спрашивает у сотрудника телевизионной компании мак-адрес оборудования (якобы чтобы помочь

данной компании) - и сотрудник сам называет его, тем самым открывая дверь хакеру.

2. При использовании почты многие делают секретным вопросом "девичья фамилия матери" - тогда хакер звонит жертве и представляется сотрудником социальной(опрашиваемой, государственной, муниципальной и др.) службы, проводит опрос о родителях - и одним из вопросов является вопрос о девичьей фамилии матери - жертва её называет и даже не предполагает что только это и нужно было злоумышленнику, т.к. человеческий мозг не сможет связать безопасность к своей почтовой системе, и опрос о родителях.

5.Защита пользователей от социальной инженерии

Нужно не только знать, как нападать, нужно знать и как защищаться

Во всех крупных компаниях регулярно проводятся тесты на проникновение с использованием социальной инженерии.

Действия сотрудников обычно носят не умышленный характер, но очень опасны для информационной безопасности. От опасности из вне можно защититься, а от опасности изнутри, практически невозможно.

С целью повышения безопасности проводятся специальные тренинги, постоянно контролируется уровень знаний и конечно же совершаются внутренние диверсии, которые позволяют выявить уровень подготовленности сотрудников в реальных условиях. Как правило, это звонки, icq, skype и электронные письма различного содержания, сервисы общения и социальные сети.

Тестирование помогает не только блокировать доступ нарушителя, но позволяет проверить реакцию сотрудников на попытки нарушения, проверить их честность.

Для защиты пользователей от социальной инженерии можно применять как технические, так и антропогенные средства.

5.1 Антропогенная защита

Простейшими методами антропогенной защиты можно назвать:

- Привлечение внимания людей к вопросам безопасности.
- Осознание пользователями всей серьезности проблемы и принятие политики безопасности системы.
- Изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения.

Данные средства имеют один общий недостаток: они пассивны. Огромный процент пользователей[1] не обращает внимания на предупреждения, даже написанные самым заметным шрифтом.

5.2Техническая защита

К технической защите можно отнести средства, мешающие заполучить информацию и средства, мешающие воспользоваться полученной информацией.

Наибольшую распространенность среди атак в информационном пространстве социальных сетей с использованием слабостей человеческого фактора получили атаки при помощи электронных писем, как то: e-mail и внутренняя почта сети. Именно к таким атакам можно с наибольшей эффективностью применять оба метода технической защиты. Помешать злоумышленнику получить запрашиваемую информацию можно, анализируя

как текст входящих писем (предположительно, злоумышленника), так и исходящих (предположительно, цели атаки) по ключевым словам. К недостаткам данного метода можно отнести очень большую нагрузку на сервер и невозможность предусмотреть все варианты написания слов. К примеру, если взломщику становится известно, что программа реагирует на слово «пароль» и слово «указать», злоумышленник может заменить их на «пассворд» и, соответственно, «ввести». Так же стоит принимать во внимание возможность написания слов с заменой кириллических букв латиницей для совпадающих символов (a, c, e, o, p, x, y, A, B, C, E, H, K, M, O, P, T, X) и использование так называемого языка t].

Средства, мешающие воспользоваться полученной информацией, можно разделить на те, которые полностью блокируют использование данных, где бы то ни было, кроме рабочего места пользователя (привязка аутентификационных данных к серийным номерам и электронным подписям комплектующих компьютера, ip и физическому адресам), так и те, которые делают невозможным(или труднореализуемым) автоматическое использование полученных ресурсов (например, авторизация по системе Captcha, когда в качестве пароля нужно выбрать указанное ранее изображение или часть изображения, но в сильно искаженном виде). Как в первом, так и во втором случае известный баланс между ценностью требуемой информации и работой, требуемой для ее получения, смещается, вообще говоря, в сторону работы, так как частично или полностью блокируется возможность автоматизации. Таким образом, даже имея все данные, выданные ничего не подозревающим пользователем, например, с целью массово разослать рекламное сообщение (спам), злоумышленнику придется на этапе каждой итерации самостоятельно вводить полученные реквизиты.

Заключение

Разговор о секретах социальной инженерии можно продолжать бесконечно, но это все равно не защитит вас от злоумышленников и мошенников всех мастей. Среди них нередко попадаются весьма талантливые люди, проворачивающие на редкость изощренные комбинации, перед которым снял бы шляпу и сам Остап Бендер. Поэтому, типовых противодействий социальным инженерам не существует и не может существовать! Каждая ситуация требует индивидуального подхода и всестороннего рассмотрения.

Единственная рекомендация - не допускайте бардака ни у себя дома, ни на работе. Расхлябанность, отсутствие дисциплины, халатность - вот главные дыры в системе безопасности, не компенсируемые ни какими, даже 1024-битными системами шифрования. Помните, что скупой платит дважды. Экономия на собственной безопасности до добра еще никого не доводила.

Список используемой литературы

1) Кевин Митник, Вильям Саймон «Искусство обмана»: Компания АйТи; 2004

2) Крис Касперски «Секретное оружие социальной инженерии»: Компания АйТи; 2005

3) Портал http://socialware.ru/

4) Домарев В. В. Безопасность информационных технологий. Системный подход — К.: ООО ТИД Диа Софт, 2004. — 992 с.

5) Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.

6) Гришина Н.В. – Организация комплексной защиты информации. – М: Гелиос АРВ, 2007. – 256.

7) Козиол Дж., Личфилд Д., Эйтэл Д., Энли К. и др. Искусство взлома и защиты систем. — СПб/ Питер, 2006. — 416 с: ил.

8) Официальный сайт «Лаборотории Касперского» http://www.securelist.com/ru/